SECURING DATA IN THE NAVY MARINE CORPS INTRANET

Decru, Inc. *275 Shoreline Drive, Suite 450, Redwood City, CA 94065*

Topic Areas: Security and NMCI; New and Transformational Technologies

Sun Tzu said, “Attack him where he is unprepared, appear where you are not expected.”

This quote is particularly germane in today’s Network Centric environment. Enemies probe weaknesses, adapt to defenses, and attack. Innocent mistakes and improperly enforced or weak security practices fail to close known and unknown windows of vulnerabilities -- vulnerabilities that expose sensitive, aggregated data to exploitation. Over the centuries, military organizations have developed sophisticated doctrines to address a wide range of security concerns. Computer and network security is no different. In many ways, today’s computer and network security resembles guerrilla warfare. Largely invisible enemies launch daily attacks on nearly every major Government agency while rapidly adapting their tactics to address countermeasures. The range of acknowledged threats continues to grow. Disgruntled insiders, viruses/worms, script kiddies, cyber terrorism, and information warfare are the security concerns of today and tomorrow. Concurrently, these same agencies have migrated to highly networked computing systems, with nearly all critical functions reliant on computing resources. This evolution has delivered higher productivity, but at the same time it has created dramatically higher exposure to electronic attacks. Consequently, concern over information assurance has never been higher. Navy and Marine Corps organizations share this concern. It is particularly acute in today’s Network Centric Warfare environment when combined with the continued aggregation of data. A secure NMCI is a vital component of the Network Centric Warfare environment. Breaches and leakage of sensitive data can have unpredictable and far-reaching consequences for Sailors and Marine in harms way.

Technologies like NAS and SAN that aggregate data clearly improve scalability, manageability and access to critical data. Additionally, these technologies can simplify the process for enterprises seeking to implement comprehensive disaster recovery programs. However, data in these environments is significantly more vulnerable to unauthorized access, theft, or misuse than data stored in more traditional, direct-attached storage. Aggregated storage is not designed to compartmentalize data, thus data from different organizations is co-mingled in the network. Data backup, off-site mirroring and other disaster recovery techniques increase the risk of unauthorized access from people both inside and outside the enterprise. Access through firewalls for legitimate Government/business needs create additional vulnerabilities. Typically, organizations combat these risks by protecting the perimeter of the network. Data at the core, however, is still dangerously open to internal and external attacks. If perimeter barriers are breached then data assets are exposed. A single breach can threaten the data assets of an entire organization.

In the NMCI environment, order-of-magnitude improvements in organizational effectiveness are being realized. In this environment, the Navy and Marine Corps need to achieve a greater level of security then was achieved in the traditional “stove-piped” networks of old. Those using the NMCI must have confidence that their data is secured and only used by those that are entitled.

In our presentation, we will explore how time-tested defense principles such as defense in depth, role separation, two-man rule, need-to-know, and multi-level security (MLS) when combined with appropriate technology can be applied in the NMCI environment to prepare for this warfare and build a successful defense.